

List of supported PubkeyAcceptedKeyTypes in Ezeelogin

573 Nesvin KN January 24, 2024 [General](#) 3687

List of supported **PubkeyAcceptedKeyType**, and **KEX (Key Exchange Algorithm)**, **HostKeyAlgorithms** in ezsh shell (Ezeelogin backend shell)

Refer to the below article to find and modify the KEX and HostKeyAlgorithms in use by the sshd server.

[KEX and Host Key Algorithms in SSH](#)

Supported PubkeyAcceptedKeyType in Ezeelogin

PubkeyAcceptedKeyType supported on **Ezeelogin version 7.30.0 >=**

1. The ed25519 key generated with the passphrase on Centos 7 is not supported.
2. The PHP version should be 7.3 and above in AlmaLinux 8, RHEL8, CentOS8, and RockyLinux to save the key in the Ezeelogin GUI.
3. Refer below articles to resolve the DSA key-based authentications.
 - [DSA key-based authentication is not working](#)
 - [signature algorithm ssh-dss not in PubkeyAcceptedAlgorithms](#)

Supported Pubkey Types:

- rsa
- dsa
- ed25519
- ecdsa
- OpenSSH

Supported KEX and HostKeyAlgorithms in Ezeelogin

Below are the supported and unsupported KEX (Key Exchange) and HostKeyAlgorithms on **Ezeelogin version 7.29.11**.

Supported KEX algorithms:

- curve25519-sha256
- curve25519-sha256@libssh.org
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group14-sha256
- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1

Supported HostKeyAlgorithms:

- ecdsa-sha2-nistp256
- ssh-ed25519
- ssh-rsa
- ssh-dss
- rsa-sha2-512
- rsa-sha2-256

Unsupported HostKeyAlgorithms:

ecdsa-sha2-nistp256-cert-v01@openssh.com, ecdsa-sha2-nistp384-cert-v01@openssh.com, ecdsa-sha2-nistp521-cert-v01@openssh.com, ssh-ed25519-cert-v01@openssh.com, ssh-rsa-cert-v01@openssh.com, ssh-dss-cert-v01@openssh.com, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, sk-ecdsa-sha2-nistp256-cert-v01@openssh.com, sk-ssh-ed25519-cert-v01@openssh.com, rsa-sha2-512-cert-v01@openssh.com, rsa-sha2-256-cert-v01@openssh.com, ssh-rsa-cert-v01@openssh.com, sk-ecdsa-sha2-nistp256@openssh.com, sk-ssh-ed25519@openssh.com

Related Articles

[Upgrade Ezeelogin Jump server to the latest version](#)

[Convert existing key format to PEM format](#)

Online URL:

<https://www.ezeelogin.com/kb/article/list-of-supported-pubkeyacceptedkeytypes-in-ezeelogin-573.html>